

**A WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF OPERATION
INCLUDING HEART BEAT PROFILE BASED AUTHENTICATION**

Related Application

5 This application is a non-provisional application of provisional application 60/459,281, filed on March 31, 2003, having the same title, and claims priority to said '281 provisional application.

 Said '281 provisional application is a continuation-in-part application of U.S. Non-Provisional Patent Application 09/690,679, entitled "A Mobile Digital
10 Communication/Computing Device Including A Heart Rate Monitor", filed on October 16, 2000, and claims priority for the base materials to said '679 non-provisional application, which specification is incorporated into the '281 provisional application by reference.

 Accordingly, for the U.S. version, this application also claims priority, through
15 said '281 provisional application, to the '679 non-provisional application for the base material described in the '679 non-provisional application.

FIELD OF THE INVENTION

The present invention relates to the field of wireless communication. More specifically, the present invention is related to a wireless mobile phone having an authenticated mode of operation available only to an authenticated user, in

5 particular, a user authenticated via a heart beat profile of the user.

BACKGROUND OF THE INVENTION

Advances in microprocessor and telecommunication technology have led to wide spread deployment and adoption of mobile devices, such as wireless mobile
10 phones. For wireless mobile phones, in addition to wireless telephony, the late models are often equipped with advanced capabilities, such as calendar, address book, access to the World Wide Web (WWW), emails, and so forth.

Much of these functionalities are designed to increase the productivity of business users. As a result, it is not surprising that business users constitute a
15 major user segment of wireless mobile phones, especially for the high-end function rich models. Increasingly, more business data, such as business contact information, business plans, sales/marketing strategies, financial reports, and so forth, are being stored on wireless mobile phones.

However, unlike personal computers or other computing devices, where user
20 authentication, through e.g. user log-in, are routinely provided with virtually all operating systems, few if any operating systems of wireless mobile phones provide means to authenticate users. As a result, under the prior art, wireless mobile phones are at risk of unauthorized usage, as well as data being compromised by unauthorized accesses.

25

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references
5 denote similar elements, and in which:

Figure 1 illustrates a front view of a wireless mobile phone incorporated with the teachings of the present invention, in accordance with one embodiment;

Figures 2-3 illustrate two architectural views of the wireless mobile phone of **Fig. 1**, in accordance with one embodiment;

10 **Figures 4a-4b** illustrate the operational flow of the relevant aspects of the operating logic of **Fig. 3**, in accordance with one embodiment;

Figure 5 illustrates a front view of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with an alternate embodiment;

15 **Figures 6a-6b** illustrate two perspective views of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with yet another embodiment;

Figures 7a-7b illustrate a front view and a side view of another wireless mobile incorporated with another aspect of the teachings of the present invention, in
20 accordance with yet another embodiment; and

Figures 8a-8b illustrate a front view and a back view of the identity card of **Fig. 7b** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Embodiments of the present invention includes a wireless mobile phone having an authenticated mode of operation, available only to an authenticated user, in particular, a user authenticated by a heart beat profile of the user.

5 Parts of the description will be presented in terms commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. The term "wireless mobile phone" as used herein (in the specification and in the claims) refers to the class of telephone devices equipped to enable a user to make and receive calls wirelessly, notwithstanding the user's movement, as long as the
10 user is within the communication reach of a service or base station of a wireless network service provider. Unless specifically excluded, the term "wireless mobile phone" is to include the analog subclass as well as the digital subclass (of all signaling protocols).

 In the following description, various aspects of the present invention will be
15 described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may
20 be practiced without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention.

 Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are

necessarily order dependent. In particular, these operations need not be performed in the order of presentation.

The phrase "in one embodiment" is used repeatedly. The phrase generally does not refer to the same embodiment, however, it may. The terms "comprising",
5 "having" and "including" are synonymous, unless the context dictates otherwise.

Referring now to **Figures 1 and 3a-3b**, wherein a front view and two architecture (internal component) views of a wireless mobile phone of the present invention, in accordance with one embodiment, are shown. As illustrated, wireless
10 mobile phone **100** of the present invention (hereinafter, simply phone **100**) is advantageously provided with operating logic **240** equipped in particular with security function **242**, to operate phone **100** in at least an unauthenticated mode of operation and an authenticated mode of operation.

While operating in the unauthenticated mode of operation, i.e. without having
15 the user authenticated, operating logic **240** makes available only a limited or reduced set of functions, whereas under the authenticated mode of operation, i.e. having the user authenticated, operating logic **240** makes available a more expanded or the entire set of functions.

The exact constitution of the limited/reduced set of functions and the
20 expanded/full set of functions is application dependent, which may vary from embodiments to embodiments. In one embodiment, the limited/reduced set of functions include only the ability to make an emergency call, such as a 911 call, otherwise, no other functions, including but not limited to making other calls, accessing calendar, email, text messaging, viewing and/or storing documents, and

so forth, are permitted. These other functions are available only under the authenticated mode.

In another embodiment, the limited/reduced set of functions may effectively be a null function set, excluding even the ability to make an emergency call, except for
5 notification of the unauthenticated status of the user, and perhaps, inviting the user to authenticate himself/herself, by e.g. allowing a heart beat profile of the user to be captured in real time.

In various embodiments, in addition to the above described unauthenticated and authenticated modes of operation, operating logic **240** further supports a
10 provisioning mode of operation, under which phone **100** is initially provisioned. Under the initial provisioning mode, conventional provisioning, such as configuring phone **100** for a particular wireless carrier, a particular subscriber and so forth, may be performed. Entry into the initial provisioning mode may be effectuated in any one of a number of conventional approaches.

15 Continue to refer to **Figures 1** and **3a-3b**, for the illustrated embodiment, phone **100** is further advantageously equipped with sensors **132** to facilitate real time capturing of a heart beat profile of the user (while operating in the authenticated mode). Further, operating logic **240**, or more specifically, security function **242**, is endowed to facilitate such capture, and authenticate a user through the heart beat
20 profile of the user (prior to operating phone **100** in the authenticated mode).

In particular, as will be described in more detail below, operating logic **240**, in general, is equipped to establish a reference heart beat profile of a user for authentication purpose, and automatically invokes sensors **132** to capture a heart beat profile of the user real time, during power on or reset. Further, security function
25 **242** is endowed to use the reference and the real time captured heart beat profiles of

the user to authenticate the user, and determine whether to continue to operate phone 100 in an unauthenticated mode, or operate phone 100 in an authenticated mode.

5 In other words, under the present invention, operating logic 240 operates phone 100 in the authenticated mode, and makes available the expanded/full set of functionalities, only if the user has been authenticated by his/her heart beat profile, otherwise, phone 100 is operated in the unauthenticated mode with only a limited/reduced set of functionalities (except in the initial provisioning mode).

10 For the embodiment, sensors 132 are disposed along and underneath the side surfaces of phone 100. A dynamically determined subset of sensors 132 are employed to capture the heart beat profile of the user. The subset of sensors 132 to be employed is based on whether the user is holding phone 100 with his/her left or right hand, thereby coming into contacts with different ones of sensors 132. Discernment of the appropriate subsets of sensors 132, or more specifically, the
15 sensing data outputted by sensors 132, to be used, is described in detail in parent U.S. Patent Application number 09/690,679 set forth and incorporated by reference above.

The heart beat profile is based on the heart beat data collected over a predetermined amount of time. The length of the predetermined amount of time to
20 be employed to construct a user's heart beat profile is application dependent, and may vary from implementation to implementation.

Further, operating logic 240, more specifically, security function 242, also supports the capturing of a heart beat profile of the user, and its saving as a reference for subsequent analysis of a real time captured heart beat profile of the
25 user to authenticate the user, before operating phone 100 in the authenticated mode.

In various embodiments, the saving of the reference heart beat profile is also supported under a special configuration mode, while operating in the authenticated mode. Entry into the configuration mode (while operating in the authenticated mode) may also be effectuated in any one of a number of conventional means.

5 Before proceeding with further description of phone **100**, it should be noted that, while for ease of understanding, the present invention has been described referencing embodiments, where user authentication is substantially based on the heart beat profile of the user, in alternate embodiments, the present invention may be practiced with the user authentication being based on other user bio-metrics. An
10 example of such other user bio-metrics is the user's finger print, which may e.g. collected optically, or electronically. An example of an optical collector is a camera, whereas an example of an electronic collector is capacitance sensor.

Continuing to refer to **Fig. 1** and **3a-3b**, additionally, phone **100** includes conventional wireless telephony elements, including power switch **122**, power **222**,
15 audio communication elements, such as ear speaker **112** and microphone **114**, and non-audio communication elements, such as input key pad **102** having a number of alphanumeric input keys and display **108**. Further, the non-audio input elements may further include scroll button **105**, selection buttons **106**, and "talk" and "end talk" buttons **104**. These elements are disposed on various external surfaces of body
20 **116**.

As illustrated in **Fig. 3a**, upon depression by a user (optionally, for a predetermined duration), while phone **100** is in a powered down or lower power state, power switch **122** couples power **222** to sensors **132** and other components **202-212**. Likewise, upon depression by a user (optionally, for a predetermined
25 duration), while phone **100** is in powered up state, power switch **122** cuts off or

reduces power **222** to all or selected ones of sensors **132** and other components **202-212**.

Externally, phone **100** may also include antenna **110**. Keys of key pad **102** may be surrounded by, or otherwise include illuminable light emitting diodes (LED) in their backgrounds. For the purpose of the present specification, the terms "button" and "key" may be considered synonymous, unless the context clearly indicates otherwise.

Internally, in addition to processor **202** and DSP **204**, phone **100** also includes non-volatile memory **206**, general purpose input/output (GPIO) interface **208**, and transmit/receive (TX/RX) **212**, coupled to each other, processor **202** and DSP **204**, via bus **214**, and disposed on a circuit board **220**.

Except for the novel manner that many of these elements, such as processor **202**, DSP **204** and so forth, are used in support of making the expanded/full set of functionalities available only to an authenticated user, the enumerated elements otherwise perform their conventional functions known in the art.

Non-volatile memory **206** is employed to store programming instructions and optionally, working data, including operating logic **240** and its security function **242**. Working data may include callee/messaging party or parties (e.g. their phone numbers or IP addresses) with whom user may communicate. Working data may include the reference and input heart beat profiles of the user.

Processor **202**, assisted by DSP **204**, is employed to operate phone **100**, executing operating logic **240**, including security function **242**.

Keys of key pad **102** may be employed to enter alphanumeric data, including entering a sequence of alphanumeric data for the phone number or address of a "callee". Selected sequence of the keys (such as "**#") may also be employed to

denote a user instruction to return to the unauthenticated mode of operation, if entered while operating in the authenticated mode of operation, or to return to the authenticated mode of operation, if entered while operating in the unauthenticated mode of operation (provided the user is authenticated).

5 Scroll key **105** and companion selection keys **106** may be employed to scroll and select various options or list items of various menu options or selection lists, including scrolling and selecting list items presented for user interactions to verify the user's wellness. For the embodiment, scroll key **105** may be selected in one of two positions, an "up" position or a "down" position for scrolling a selection list in an "up" direction and a "down" direction respectively. Similarly, scroll and selection keys **105/106** may also be employed to select a menu item to convey a user instruction to return to the unauthenticated mode, if the selection is made while operating in the authenticated mode, or to return to the authenticated mode, if the selection is made while operating in the unauthenticated mode (provided the user is authenticated).

10 GPIO **208** may be employed to generate input signals, such as a corresponding "alphanumeric" signal in response to a user selection of one of the keys of key pad **102**, a "scroll" signal" (or more specifically, a "scroll up" or a "scroll down" signals) in response to a user selection of scroll key **105**, a "selection" signal in response to a user selection of select button **106**, and so forth.

15 TX/RX **212** may be employed to transmit and receive communication signals for a call and/or a text message. TX/RX **212** may be a radio frequency transceiver, and support one or more of any of the known signaling protocols, including but are not limited to CDMA, TDMA, GSM, and so forth.

20 The constitutions of these elements are known, and will not be further described.

As to operating logic **240**, including security function **242**, it may be implemented in the assembly or machine instructions of processor **202**, or a high level language that can be compiled into these assembly or machine languages. In alternate embodiments, all or portions of operating logic **240**, including security
5 function **242** may be implemented in firmware and/or hardware.

Accordingly, except for the enhancements provided, phone **100** otherwise represents a broad range of wireless mobile phones, including both the analog as well as the digital types (of all signaling protocols), substantially rectangular uni-body as illustrated, or curved uni-body, as well as multi-portions, such as "flip phones" to
10 be illustrated later.

Figure 4 illustrates the operational flow of the relevant aspects of operating logic **240**, in accordance with one embodiment. As illustrated, on start up/reset (such as depression of power on/off button **122** for the required predetermined
15 duration by a user), operating logic **240** enables phone **100** to operate in the earlier described unauthenticated mode, making available only a limited/reduced set of functionalities, block **402**. Thereafter, operating logic **240** waits for additional user input, block **404**.

Recall from earlier description, upon depression by a user, while phone **100** is
20 in powered down or low power state, power switch **122** couples power to sensors **132** and other components **202-212** of phone **100**. For the embodiment, on power on/reset, operating logic **230** causes sensors **132** to sense the heart beat pattern of the user, based on the user's fingers **250** in contact. Resultantly, after a predetermined elapsed amount of time, a heart beat profile of an authorized user
25 who is aware of the authentication requirement, and have properly held the phone

with his/her fingers in contact with sensors **132**, would have a heart beat profile of the user taken or captured in real time, for authentication.

Accordingly, under the present invention, heart beat profile based authentication is seamlessly integrated with the power on/reset process.

5 Continuing to refer to **Fig. 4**, on receipt of inputs, operating logic **240** determines if the input is a heart beat profile captured by sensors **132** in real time (more specifically, by DSP **204**, after it processes the signals output by sensors **132** into a heart beat profile), block **406**.

10 If the user input is a heart beat profile, operating logic **240** (or more specifically, security function **242**) further determines if phone **100** is operating in the unauthenticated mode, within the authenticated mode (including whether it is within the configuration mode of the authenticated mode), or the initial provisioning mode, block **407**.

15 If phone **100** is determined to be operating in the configuration mode within the authenticated mode, or the initial provisioning mode, operating logic **240** (or more specifically, security function **242**) saves the captured heart beat profile as a reference heart beat profile for future user authentication, block **408**.

20 If phone **100** is determined to be operating in the unauthenticated mode, operating logic **240** (or more specifically, security function **242**) initiates the heart beat profile based authentication process, authenticating the user by comparing the real time captured heart beat profile, against the previously saved reference heart beat profile, block **409**.

If the heart beat profile does not substantially match the previously saved reference heart beat profile, block **410**, operating logic **240** (or more specifically,

security function **242**) reports the authentication failure, block **412**, and continues to operate phone **100** in the unauthenticated mode at block **404**.

However, if the inputted heart beat profile substantially matches the previously saved reference heart beat profile, block **410**, operating logic **240** (or more specifically, security function **242**) enables phone **100** to operate in the authenticated mode, block **414**. Thereafter, operating logic **240** continues operation at block **404**.

The precision level at which a real time captured heart beat profile is to be considered substantially matching with a reference heart beat profile is application dependent. Preferably, different user selectable precision levels are offered. As with other user selectable options, the selection may be facilitated in any one of a number of known user selection techniques.

Back at block **408**, if the input is determined not to be heart beat profile input, operating logic **240** determines if the input is a user instruction to return to the unauthenticated mode of operation (e.g. a user selecting or inputting such command using alphanumeric keys **102** and/or scroll/select keys **105** and **106** while operating in an authenticated mode of operation), block **416**.

If the input is determined to be a user instruction to return to the unauthenticated mode of operation, operating logic **240** (or more specifically, security function **242**) returns phone **100** to operate in the unauthenticated mode, block **418**. Thereafter, operating logic **240** continues operation at block **404**.

In one embodiment, before exiting to the unauthenticated mode, operating logic **240** (or more specifically, security function **242**) causes a user selectable "resume" (i.e. re-authentication) option to be rendered on display **108**. Selection of the option is processed as if phone **100** is being powered on or reset. That is,

operating logic **240** automatically causes sensors **132** to capture another heart beat profile of the user for authentication purpose.

If the input is determined to be other user inputs, operating logic **240** handles the other user inputs in an application dependent manner, block **420**. In particular, if
5 the input is a user instruction to return to the authenticated mode of operation, operating logic **240** continues operation at block **404**, and awaits for another heart beat profile input to re-authenticate the user. If the input is other conventional inputs, the inputs are processed as in the prior art. Thereafter, operating logic **240** continues operation at block **404**.

10 **Figure 5** illustrates another embodiment of the wireless mobile phone of the present invention. More specifically, **Fig. 5** illustrates a front view of the alternate embodiment. The alternate embodiment is substantially that of the embodiment of **Fig. 1**, except that phone **100** is substantially rectangular in shape, whereas phone
15 **500** has a curved shape.

Figures 6a-6b illustrate yet another embodiment of the wireless mobile phone of the present invention. More specifically, **Fig. 6a-6b** illustrate two perspective views of the embodiment. The embodiment is also substantially that of the
20 embodiments of **Figs. 1** and **5**, except that phone **100** is substantially rectangular, phone **500** has a curve shaped body, whereas phone **700** has a multi-section body. The multi-section form factor includes a first section **716b** and a second section **716c**, and the second section **716c** is further comprised of at least two sub-sections **716d-716e**. The first and second sections **716b-716c** may pivot towards each other
25 as denoted by direction arrow **706a** or away from each other opposite to the direction

denoted by arrow **706a**. Sub-section **716d** may rotate relative to sub-section **716e** as denoted by the directions denoted by arrows **706b**. In other words, phone **700** may be considered as an improved version of what is commonly referred to as "flip" phones.

5 Similar to the earlier described embodiments, phone **700** is provided with operating logic having a security function as earlier described, and sensors **732**.

 In alternate embodiments, second section **716c** may be a uni-section, i.e. it is not further sub-divided into to relatively pivotable sub-sections.

10 In yet other embodiments, the reference heart beat profile may be provided to the wireless mobile phone in a secure manner, e.g. read from an identity card, via an identity card reader additionally provided to the wireless mobile phone.

Figures 7a-7b illustrate one such embodiment. As illustrated in **Fig. 7b**, wireless mobile phone **100** is additional endowed with an identity card reader **740**.
15 Identity card reader **740** (optionally, assisted by a device driver additionally provided to supplement operating logic **240**) is equipped to retrieve the earlier described reference heart beat profile from identity card **742**.

 Preferably, identify card **742** has a form factor that is difficult to forge, and its issuance is governed by a secured process. Resultantly, security for wireless mobile
20 phone **100** is further enhanced.

 For the embodiment, identity card **742** comprises a smart electronic card **744** (commonly referred to as a smart card) (see **Fig. 8a-8b**), and the reference heart beat profile is pre-stored in the embedded smart card **744**. Operating logic **240** (optionally, supplemented by a corresponding reader device driver) retrieves the

reference heart beat profile from embedded smart card **744**, on detection of the presence of identity card **742**.

In various embodiments, the reference heart beat profile may be further protected via encryption, requiring operating logic **240** to possess the proper
5 decryption key to recover the reference heart beat profile after retrieval.

In yet other embodiments, the reference heart beat profile may be further protected via an authentication protocol, requiring wireless mobile phone **100** to be equipped with the appropriate credential to authenticate itself to smart card **744**, before being allowed by smart card **744** to access the pre-stored reference heart
10 beat profile in smart card **744**.

In yet other embodiments, the reference heart beat profile may be imprinted on identity card **742**, and identity card reader **720** is an optical reader.

In yet still other embodiments, the reference heart beat profile may be encoded via a magnetic strip disposed on a surface of identity card **742**, and identity
15 card reader **720** is a magnetic code reader.

In yet still other embodiments, the reference heart beat profile may be stored in a storage that is removably attached to the wireless mobile phone **100**. An example of a suitable removable storage is a flash memory based device.

These are just a few example, other equivalent encoding/storing and
20 reading/retrieving techniques may also be employed instead.

Conclusion and Epilogue

Thus, it can be seen from the above descriptions, a novel wireless mobile phone that can afford protection against unauthorized access to user data and/or
25 usage of the phone, using bio-metric based authentication, has been described.

While the present invention has been described in terms of the foregoing embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims.

5 In particular, the present invention may be practiced with employing additional and/or other means to authenticate a user.

Thus, the description is to be regarded as illustrative instead of restrictive on the present invention.

10